

REMARKS

The Applicants gratefully acknowledge potential allowability of claims 23-33 and 53-55.

The present patent application now comprises fifty (50) claims, numbered 1-10, 12-15, 18-50 and 53-55.

Claims 1, 7, 12, 13, 15, 18, 24, 37, 49, 50 and 53-55 have been amended to clarify the subject matter being claimed. Claims 11, 16, 17, 51 and 52 have been cancelled without prejudice. Non-elected claims 56-60 have also been cancelled without prejudice.

Support for amendments made can be found throughout the specification and drawings as originally filed. It is believed that no new matter has been added to the application by the present response.

1. Objection to Claims 24, 37 and 49-51

On page 3 of the Office Action, the Examiner objects to certain claims of the application. Specifically:

- The Examiner appears to object to claim 51 due to presence of the phrase “sending a message to the end user device instrumental in causing the end user device to” since he considers that the term “instrumental” is a subjective term. In response, the term “instrumental” has not been included in each of claims 53-55 that incorporates the subject matter of claim 51, which has been cancelled.
- The Examiner objects to claim 37 since the expression “the user interface” lacks antecedent basis, and to claim 49 since the expressions “the server” and “the memory store” lack antecedent basis. In response, claims 37 and 49 have been amended to overcome this lack of antecedent basis.

- The Examiner objects to claim 24 since he considers that the expression “proximate the end user device” should read “proximate to the end user device”. In response, claim 24 has been amended to read “proximate to the end user device”.
- The Examiner objects to claim 50 since he considers that it misses a comma. It is assumed that the Examiner meant that claim 50 misses a period at its end. Accordingly, a period has been added at the end of claim 50.

The Examiner also considers that it is not clear how specifying that the sensitive information comprises healthcare information limits claim 49, from which claim 50 depends. With respect, the Applicants respectfully disagree. Specifically, while the sensitive information referred to in claim 49 can be any type of sensitive information, claim 50 specifies that the sensitive information comprises healthcare information, i.e., clinical data or other information pertaining to healthcare. Thus, claim 50 is a proper dependent claim and is in no need of any amendment.

In light of the above, it is respectfully submitted that the Examiner’s objections to claims 24, 37 and 49-51 have been addressed and overcome. The Examiner is therefore respectfully requested to withdraw the objections to these claims.

2. Rejection of Claims 7 and 52 under 35 USC 112

On pages 4 and 5 of the Office Action, the Examiner rejects claim 52 under 35 USC 112, first and second paragraphs. Specifically, the Examiner considers that it is not clear how the end user device receives the message after the session is terminated.

This rejection is moot in view of cancellation of claim 52. However, for completeness, it is respectfully submitted that claim 52, prior to its cancellation, fully complied with 35 USC 112, first and second paragraphs. Specifically, a message such as a session termination

message can be sent to the end user device and received at its network interface upon detection of termination of the session, as described in the specification, *inter alia*, at p. 14, lines 23-26, p. 15, lines 23-34, p. 18, lines 15-23 and p. 19, lines 2-13.

The Examiner also rejects claim 7 under 35 USC 112, second paragraph, as being unclear due to the expression “a host” in both claim 7 and its base claim (claim 6). In response, claim 7 has been amended to be dependent on claim 5, which does not contain the expression “a host”.

In light of the above, it is respectfully submitted that the Examiner’s rejections under 35 USC 112 have been addressed and overcome. The Examiner is therefore respectfully requested to withdraw the rejection of claim 7 under 35 USC 112.

3. Rejection of Claims 15-22 and 34-51 under 35 USC 102 or 103

On pages 6 to 11 and 13 to 15 of the Office Action, the Examiner rejects claims 15-22 and 34-51 under 35 USC 102(b) and/or 35 USC 103(a) as being anticipated by and/or obvious over various references. Specifically:

- the Examiner rejects claims 15-22, 34, 36, 37, 49 and 50 under 35 USC 102(b) as being anticipated by or, alternatively, under 35 USC 103(a) as being obvious over Windows NT/2000 as illustrated by Jeff Schmidt in “Microsoft Windows 2000 Security Handbook”, ISBN 0789719991, August 2000 (hereinafter referred to as “Schmidt”);
- the Examiner rejects claims 15, 16, 35, 36 and 44-51 under 35 USC 102(b) as being anticipated by or, alternatively, under 35 USC 103(a) as being obvious over Windows 2000 as illustrated by Microsoft TechNet in “Data Protection Implementing the Encrypting File System in Windows 2000” posted in “Windows 2000 File Systems Tutorials”, in particular “Step-by-Step Guide to Encrypting File System (EFS) article in May 2002 (hereinafter referred to as “Microsoft TechNet”); and

- the Examiner rejects claims 38-43 under 35 USC 103(a) as being obvious over Windows 2000 as illustrated by Microsoft TechNet in view of U.S. Patent 5,677,952 to Blakley, III *et al.* (hereinafter referred to as “Blakley”) and Bruce Schneier in “Applied Cryptography, Protocols, Algorithms and Source Code in C”, 2nd edition, ISBN 0471128457, 1996 (hereinafter referred to as “Schneier”).

As discussed below, it is respectfully submitted that claims 15, 18-22 and 34-50, as amended, are in allowable form and the Examiner is respectfully requested to withdraw his objections to these claims.

Claims 15, 18-22 and 34-48

Claim 15 has been amended to include elements previously claimed in claims 16 and 17, which are now cancelled. For ease of reference, claim 15 is reproduced below with certain portions being emphasized:

An end user device for communication with a server, comprising:

- a control entity operative to support a session with the server for **an authenticated user**;
- a memory store operative to store sensitive information during the session;
- a user interface for interfacing with the authenticated user; and
- a network interface for interfacing with the server;
- the control entity further operative to (i) **apply a policy based on stimuli received via the user interface and the network interface to determine whether confidentiality of the sensitive information stored in the memory store is to be preserved** and (ii) responsive to determining that confidentiality of the sensitive information stored in the memory store is to be preserved, take an action to preserve confidentiality of the sensitive information stored in the memory store.

It is respectfully submitted that Schmidt, Microsoft TechNet, Blakley and Schneier, whether taken individually or in combination, neither anticipate nor render obvious an end user device comprising a control entity operative to: support a session with a server for an authenticated user; apply a policy based on stimuli received via a user interface and a network interface to determine whether confidentiality of sensitive information stored in a memory store during the

session is to be preserved; and, responsive to determining that confidentiality of the sensitive information stored in the memory store is to be preserved, take an action to preserve confidentiality of the sensitive information stored in the memory store.

Specifically, none of the cited references teaches or suggests a control entity of an end user device being operative to apply a policy based on stimuli received via a user interface and a network interface in order to determine whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved.

– Schmidt and Microsoft TechNet –

Schmidt and Microsoft TechNet's discussions of Windows NT/2000 in no way show that Windows NT/2000 causes an end user device to apply a policy based on stimuli received via its user interface and network interface in order to determine whether confidentiality of sensitive information stored in a memory store during a session for an *authenticated user* is to be preserved. Specifically, there is no mention or suggestion in Schmidt and Microsoft TechNet of application of any kind of "policy" that is based on stimuli received via an end user device's user interface and network interface in order to make a determination as to whether confidentiality of sensitive information stored in a memory store during a session for an *authenticated user* is to be preserved.

This is true for Schmidt and Microsoft TechNet's discussions of Windows NT/2000 in general and in particular for the functionality of Windows NT/2000 referred to by the Examiner. More particularly:

- The functionality of Windows NT/2000 pertaining to "The General Logon Sequence", "Authentication Procedure" and "Account Lockout Policy" discussed in Schmidt (pp. 320-322 and p. 560) relates to functionality invoked before a user is authenticated. Indeed, the Windows NT/2000 functionality allowing a user to enter the Ctrl+Alt+Del command and then his/her username and password as well as the Windows NT/2000 functionality

preventing the user from being authenticated after a certain number of incorrect logons is functionality invoked before the user is authenticated. It is therefore abundantly clear that this functionality in no way amounts to a determination as to whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved, i.e., a determination made in a case where *a user has been authenticated*.

- The functionality of Windows NT/2000 discussed in Microsoft TechNet in the section "Encrypting a file or folder" relates to functionality allowing a user to select a file or folder to be encrypted. In other words, this allows the user, not his/her end user device, to determine which file or folder is to be encrypted. Clearly, therefore, this functionality in no way amounts to an end user device's control entity applying a policy to determine whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved.
- The functionality of Windows NT/2000 discussed in Schmidt and Microsoft TechNet relates to an end user device operating based on input from a user (e.g., the user entering the Ctrl+Alt+Del command and his/her username and password, the user selecting a file or folder to be encrypted). However, this functionality in no way involves the end user device making a determination based on stimuli received via a network interface. Therefore, this functionality in no way amounts to an end user device applying a policy based on stimuli received via its user interface and network interface in order to make any kind of determination, let alone a determination as to whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved.

Thus, Schmidt and Microsoft TechNet fail to show that Windows NT/2000 causes an end user device to apply a policy based on stimuli received via its user interface and network interface in order to determine whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved. In fact, on page 11 of the

Office Action, the Examiner concedes that “[i]n Windows 2000 it is a user that determines whether confidentiality of the sensitive information is to be preserved” (emphasis added), and thus not his/her end user device.

– Blakley –

Blakley describes a device driver on a computer to protect information stored in a storage device of the computer, where the device driver encrypts and decrypts all accesses to and from the storage device (col. 3, lines 20-25 and 34-40, and col. 4, line 66 and 67). There is absolutely no mention or suggestion in Blakey of the device driver being operative to make any kind of determination as to whether confidentiality of sensitive information stored in the storage device during a session for an authenticated user is to be preserved. In fact, there is no need for such a determination in Blakley since the device driver encrypts and decrypts all accesses to and from the storage device. Accordingly, it is ample clear that Blakey fails to teach or suggest an end user device’s control entity being operative to apply a policy based on stimuli received via a user interface and a network interface in order to determine whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved.

– Schneier –

Schneier discusses in a general manner encryption effected using hardware and software (pp. 223-225). There is absolutely no mention or suggestion in Schneier of making any kind of determination as to whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved. As such, Schneier cannot possibly be held to teach or suggest an end user device’s control entity being operative to apply a policy based on stimuli received via a user interface and a network interface in order to determine whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved.

In view of the foregoing, Schmidt, Microsoft TechNet, Blakley and Schneier, whether taken individually or in combination, fail to teach or suggest at least one element of claim 15. This failure of the cited art to teach or suggest at least one claimed element precludes a finding of anticipation or obviousness in respect of claim 15.

In addition, the Examiner failed to identify an apparent reason why an ordinarily skilled person looking at the cited art would be led to the claimed end user device, which comprises a control unit operative to apply a policy based on stimuli received via its user interface and network interface in order to determine whether confidentiality of sensitive information stored in a memory store during a session for an authenticated user is to be preserved. On the contrary, as mentioned above, the Examiner recognizes that, in Windows NT/2000 as illustrated by Schmidt and Microsoft TechNet, it is a user, and thus not his/her end user device, that determines whether confidentiality of sensitive information is to be preserved. This failure of the Examiner to identify an apparent reason why an ordinarily skilled person looking at the cited art would be led to the claimed end user device further precludes a finding of obviousness in respect of claim 15.

For these reasons, it is respectfully submitted that Schmidt, Microsoft TechNet, Blakley and Schneier neither anticipate nor render obvious an end user device as claimed in claim 15. The Examiner is therefore respectfully requested to withdraw the rejection of claim 15, which is believed to be allowable. Claims 18-22 and 34-48 depend on claim 15 and are thus also believed to be allowable.

Claims 49 and 50

Claim 49 is reproduced below with certain portions being emphasized:

A method comprising

- supporting a session with a server for **an authenticated user**;
- storing sensitive information during the session;

- **applying a policy based on stimuli received via a user interface and a network interface to determine whether confidentiality of the sensitive information is to be preserved;**
- responsive to determining that confidentiality of the sensitive information is to be preserved, taking an action to preserve confidentiality of the sensitive information.

The above-emphasized portions of claim 49 reflect portions of claim 15 that have been discussed above. Hence, for reasons similar to that discussed above in respect of claim 15, it is respectfully submitted that Schmidt, Microsoft TechNet, Blakley and Schneier, whether taken alone or in combination, neither anticipate nor render obvious a method as claimed in claim 49. The Examiner is therefore respectfully requested to withdraw the objection to claim 49, which is believed to be allowable. Claim 50 depends on claim 49 and is thus also believed to be allowable.

4. Rejection of Claims 1-14 under 35 USC 103

On pages 11 to 13 and 15 to 17 of the Office Action, the Examiner rejects claims 1-14 under 35 USC 103(a) as being obvious over two combinations of references. Specifically:

- the Examiner rejects claims 1-3 and 8-10 under 35 USC 103(a) as being obvious over U.S. Patent 5,677,952 to Blakley, III *et al.* (hereinafter referred to as “Blakley”) and Bruce Schneier in “Applied Cryptography, Protocols, Algorithms and Source Code in C”, 2nd edition, ISBN 0471128457, 1996 (hereinafter referred to as “Schneier”); and
- the Examiner rejects claims 1-14 under 35 USC 103(a) as being obvious over “How Computers Work” by Ron White, 7th edition, ISBN 0789730332, October 2003 (hereinafter referred to as “White”) in view of U.S. Patent 6,963,979 to Fairclough *et al.* (hereinafter referred to as “Fairclough”).

As discussed below, it is respectfully submitted that claims 1-10 and 12-14, as amended, are in allowable form and the Examiner is respectfully requested to withdraw his objections to these claims.

Claim 1 has been amended to include elements previously claimed in claim 11, which is now cancelled. For ease of reference, claim 1 is reproduced below with certain portions being emphasized:

A data processing apparatus, comprising:

- a memory store;
- a data bus connected to the memory store, the data bus being adapted for transporting data to and from the memory store;
- a processing entity operative to release read and write commands towards the memory store, the write command being accompanied by first data intended to be written to the memory store;
- an encryption module communicatively coupled to the processing entity and to the data bus;
 - upon the processing entity releasing a write command accompanied by said first data, the encryption module being operative to encrypt, in accordance with an encryption key, said first data and send an encrypted version of said first data onto the data bus for writing into the memory store;
 - upon the processing entity releasing a read command, the encryption module being operative to decrypt, in accordance with a decryption key, an encrypted version of second data received from the memory store via the data bus and provide said second data to the processing entity;
- a selection module connected between the processing entity and the encryption module, the selection module also being connected to the memory store, **the selection module being capable of selectively operating in a selected one of a first operational state in which said first and second data is exchanged directly with the memory store and a second operational state in which said first and second data is exchanged with the encryption module.**

It is respectfully submitted that Blakley, Schneier, White and Fairclough, whether taken separately or in combination, do not render obvious a data processing apparatus comprising a selection module capable of selectively operating in a selected one of a first operational state in which data to be written to or received from a memory store is exchanged directly with the memory store and a second operational state in which data to be written to or received from the memory store is exchanged with an encryption module. In other words, Blakley, Schneier, White and Fairclough do not render obvious a data processing apparatus comprising a

selection module that allows data to be selectively exchanged either with an encryption module or directly with a memory store, bypassing the encryption module. As mentioned in the present specification (see, *inter alia*, p. 22, lines 19-30), such a selection module may allow unencrypted data (e.g., data for which it is not necessary to preserve confidentiality) to be stored in the memory store and may also provide other benefits (e.g., rendering cracking of a cryptographic key more difficult, reduce delays in writing and/or reading data to/from the memory store).

– Blakley –

Blakley describes a device driver on a computer to protect information stored in a storage device of the computer. Blakley's device driver encrypts and decrypts all accesses to and from the storage device. That is, Blakley's device driver is designed such that "[t]he information obtained from each read of the storage device is decrypted, and the information obtained from each write is encrypted" (emphasis added – col. 3, lines 20-25 and 34-40, and col. 4, line 66 and 67). As such, Blakley fails to teach or suggest a selection module capable of selectively exchanging data either with its device driver for encryption/decryption or directly with the storage device, bypassing the device driver. In fact, since Blakley's device driver is designed to encrypt and decrypt all accesses to and from the storage device, Blakley actually *teaches away* from a selection module capable of selectively operating in a selected one of a first operational state in which data is exchanged directly with a memory store and a second operational state in which data is exchanged with an encryption module, as claimed in claim 1.

– Schneier –

Schneier discusses in a general manner encryption effected using hardware and software (pp. 223-225). Unsurprisingly, therefore, Schneier is totally devoid of any mention or suggestion of a selection module capable of selectively operating in a selected one of a first operational state in which data is exchanged directly with a memory store and a second operational state in which data is exchanged with an encryption module, as claimed in claim 1.

– White –

White discusses in a general manner certain basic components of a computer such as a CPU, a bus, etc. (pp. 16-18, 28 and 29). White is totally unconcerned with encryption and thus fails to contemplate any kind of encryption module. It thus goes without saying that White provides absolutely no mention or suggestion of a selection module capable of selectively operating in a selected one of a first operational state in which data is exchanged directly with a memory store and a second operational state in which data is exchanged with an encryption module (which is not even contemplated in White), as claimed in claim 1.

– Fairclough –

Fairclough describes a cryptographic accelerator comprising a host interface for interfacing with a host server requesting cryptographic operations, as well a CPU, a block cipher function, a modular exponentiation subsystem, a random number generator and a key storage function that implement encryption and decryption operations (col. 3, lines 42-56).

Fairclough's cryptographic accelerator in no way comprises a selection module capable of selectively exchanging data either with an encryption module or directly with a memory store, bypassing the encryption module. This is not surprising since the whole point of Fairclough's cryptographic accelerator is to perform cryptographic operations, not allow data to be exchanged directly with a memory without being encrypted/decrypted. In fact, as Fairclough's cryptographic accelerator is dedicated to performing cryptographic operations, Fairclough *teaches away* from a capability to selectively exchange data either with an encryption module or directly with a memory store, bypassing the encryption module's cryptographic operations.

In rejecting former claim 11, which pertained to the claimed selection module, the Examiner states that he "considers object 15, in Fig. 1 to read on selection/control module, and as it is clear from Fig. 1, any cryptographic data (keys) handled by the encryption module is received

from the selection/control module, and a signal received by the selection/control module indicates the need to exchange data (an encryption state) with the encryption module”.

Notwithstanding the lack of clarity in the Examiner’s statement, it is respectfully submitted that “object 15” in Blakley’s Figure 1 in no way amounts to the claimed selection module. Specifically, reference numeral 15 refers to a “daemon and APIs” executing on a host server that requests cryptographic operations to be performed by Blakley’s cryptographic accelerator. These daemon and APIs, as well as any other component of Blakley’s cryptographic accelerator, do not allow data to be selectively exchanged either with an encryption module or directly with a memory store, bypassing the encryption module. Rather, these daemon and APIs, like every other component of Blakley’s cryptographic accelerator, are used to perform cryptographic operations and do not allow data to be exchanged directly in a memory without being encrypted/decrypted.

In view of the foregoing, Blakley, Schneier, White and Fairclough, whether taken individually or in combination, fail to teach or suggest the claimed selection module. This failure of the cited art to teach or suggest at least one claimed element precludes a finding of obviousness in respect of claim 1. In addition, since Blakley and Fairclough each *teach away* from the claimed selection module, it is clear that neither of these references can be used to support a contention of obviousness in respect of claim 1.

For these reasons, it is respectfully submitted that Blakley, Schneier, White and Fairclough do not render obvious a data processing apparatus as claimed in claim 1. The Examiner is therefore respectfully requested to withdraw the rejection of claim 1, which is believed to be allowable. Claims 2-10 and 12-14 depend on claim 1 and are thus also believed to be allowable.

5. Objection to Claims 53-55

On page 17 of the Office Action, the Examiner indicates that each of claims 53-55 is objected to as being dependent on a rejected base claim, but would be allowable if rewritten in independent form including all of the elements of its base claim and any intervening claim.

Each of claims 53-55 has been rewritten in independent form, including the elements of base claim 51, which has been cancelled. Accordingly, in view of the Examiner's remarks regarding potential allowability of claims 53-55, it is respectfully submitted that these claims are in allowable form.

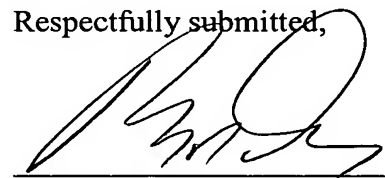
CONCLUSION

Claims 1-10, 12-15, 18-50 and 53-55 are believed to be in condition for allowance. Favorable reconsideration is requested. Allowance of the present patent application is earnestly solicited.

If the claims of the present patent application are not considered to be in full condition for allowance, for any reason, the Applicants respectfully request the constructive assistance and suggestions of the Examiner in drafting one or more acceptable claims or in making constructive suggestions so that the application can be placed in allowable condition as soon as possible and without the need for further proceedings.

Dated: 12/07/2007

Respectfully submitted,



Ralph A. Dowell
Reg. No. 26,868
Attorney for the Applicant

DOWELL & DOWELL, P.C.
2111 Eisenhower Avenue
Suite 406
Alexandria, VA 22314
U.S.A.

Telephone: (703) 415-2555
Facsimile: (703) 415-2559